MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

# VISUAL SECRETE SHARING USING NATURAL IMAGES

[1]Sayali Ekhe,[2]Nita Kokat,[3]Tejaswini Kagade
Department of Computer Engineering
Marathwada Mitra Mandal's College of Engineering,
Pune, India
[1]sayaliekhe@gmail.com,[2]nitakokat@yahoo.com,[3]tejaswinikagade@gamil.com

***Abstract:*** *Traditional cryptography is a method of converting secrete message into unreadable formats by using some keys. This cipher text can be shared through the network without fear. But there occurs some problems using this method like anyone can obtain message easily by applying key on cipher text. Another method is Visual Cryptography is a one of the encryption technique which is used to hide the information and data in image. This method uses two transparent images. One image contains random pixel and other image contains secrete information. Images are partition into n shares and they get encoded and then stored in digital format. The shares can appear as noise like pixels or as meaningful images; but it will arouse suspicion and increase transmission risk. So, Visual Cryptography suffers from a transmission risk problem for the secrete itself. Hence to address this problem NVSS (Natural Visual Secrete Sharing) can be used. The proposed NVSS (n,n) scheme can share secrete image over (n-1) natural images(called natural shares). This paper shows the anticipation that image sharing with NVSS is promising.*

***Keywords:*** *Visual Cryptography, transmission risk, Visual secret sharing scheme, natural images, secrete shares, Data Hiding, NVSS scheme.*

## 1. INTRODUCTION

Cryptography is method of storing and transmitting data in particular form so that only those for whom it is intended can read and process it. The term used for scrambling plaintext(ordinary text) into cipher text(a process called encryption),then back again Into plain text(called decryption).A visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into shares distributed to

participants[5]. If anyone gets some parts then can easily get the information which is in the secrete image. There are various types of secrete images like handwritten document, photos, images etc. Sharing this encrypted secrete images is called as visual secrete sharing (VSS) schemes. Visual secrete sharing is one of the important issue today. Main drawback of VSS is transmission risk. This paper uses the VSS by using natural images reduce transmission risk.

### 1.1. VSS Scheme

In 1994 Moni Naor and Adi Shamir developed the visual cryptography method in which the image can be secured; here image is nothing but the simple plain text. This image is divided into N parts which are called as shares this process is also called as pixel expansion and this process is a part of encryption. These shares are transmitted to the participants over the network. The participants can decode the encrypted image by taking shares orderly that „n" shares which will reveal the secret image. The shares are the secret key „k" that is basically distributed to „n" participants, the secret can be reconstructed only if the „k" shares are stacked together [6].

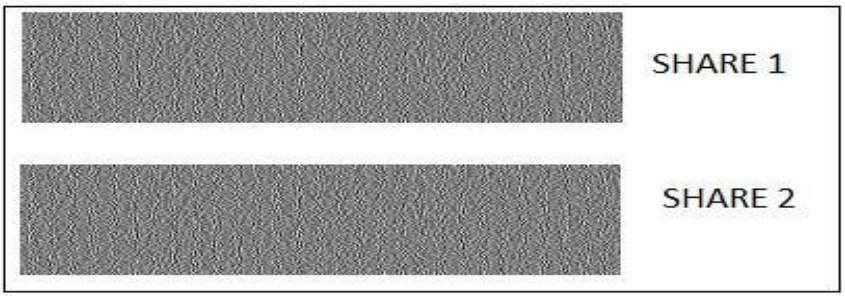



*Fig.1: Encryption*


*Fig.2: Decryption*

### 1.2. Drawbacks of Visual Secrete Sharing

The major drawback of (VSS) scheme is that it suffers from high transmission risk as the shares are like noise which causes the attackers attention and the shares can be intercepted[7].The VSS scheme is not user friendly [7].VSS scheme require the knowledge of cryptography to user.

## 3. LITERATURE SURVEY

- The author proposed that," Visual secrete sharing by using natural images is used to send the secrete image through various carrier media which includes secrete image, n-1 natural images and one noise-like share.

- The main aim of our system is to securely transfer the secrete images. The natural share can be in the form of photos or pictures in digital form and noise-like share is obtained from the natural shares and secrete image itself.
- In the existing system the noise-like shares cause the attackers suspicion so that shares may be intercepted and meaningless shares are not user friendly as increasing number of shares increases the complexity to manage these shares [1]-[4].
- In VSS scheme shares that contains many noise-like pixels and low quality images can be easily detected by necked eyes so the participants can lead to suspicious attacks. The VSS scheme is similar to OTP encryption system [1].
- In NVSS only one share is noise-like and all other are natural shares so that the risk of intercepted get reduced. We are using the different media to transfer the share which increases the difficulty of shares being intercepting.
- Also we are exacting the features from natural images without altering them so that these natural shares are totally innocuous, this reduces the interception risk. The generated noise-like share can be concealed using any data hiding technique to increase security.

## 4. PROPOSED SYSTEM

NVSS (Natural Visual Secrete Sharing) is a technique used to reduce transmission risk problems involved in secretes sharing. NVSS uses natural images instead of using noise like shares. It also used different media to transmit this will make the catch of the data difficult.

### 4.1. Image Preprocessing

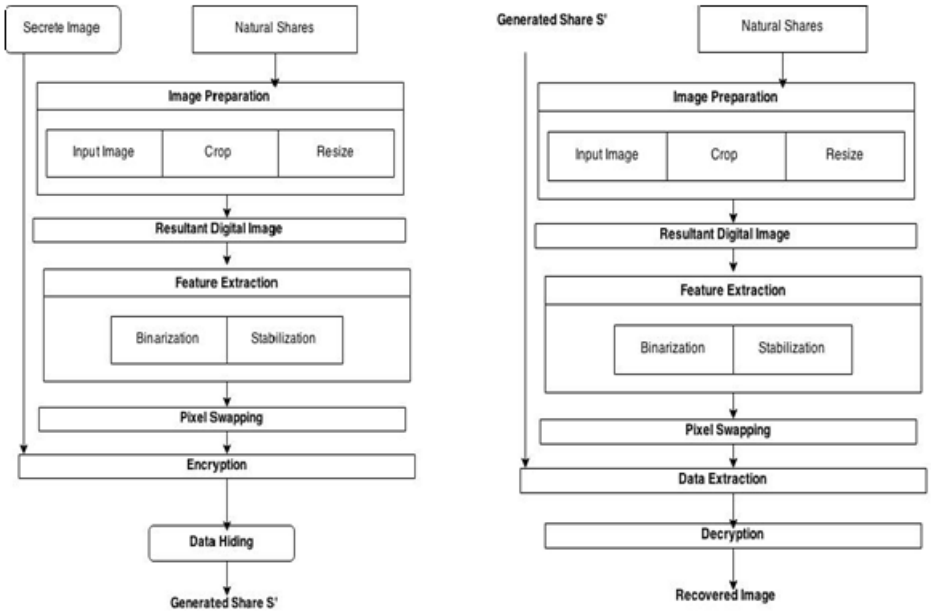
Images are of different sizes, there is a need of same size images. For that purpose cropping of original image is done, and it gives required size image. And this image used for feature extraction process.

### 4.2. Feature Extraction Process

In feature extraction process some features are extracted from natural images using Wave Transform Method. Wave Transform is a mathematical method for compressing the image and for processing the digital image.

### 4.3. Feature Extraction Process

In feature extraction process some features are extracted from natural images using Wave Transform Method. Wave Transform is a mathematical method for compressing the image and for processing the digital image. Feature extraction has processes includes binarization, stabilization. A simple threshold function F is used to determine the binary feature value of the pixel. This process is called as binarization. The extracted feature of each block is balanced using stabilization process, i.e. black and white pixels of each block are balanced. And then disordering the original matrix noise gets added to it. This process is called as Chaos process.




*(a)Encryption Process.* *(b)Decryption Process.*

*Fig.3: Encryption-Decryption Process.*

### 4.4. Pixel Swapping Process

Pixel swapping is done in order to add randomness to the image. Two pixels are picked from random column and swapped if upper pixel has higher hue. The pixels of the random row are selected and swapped so the left pixel will have higher brightness than the right. This process gets repeated on the complete image.

### 4.5. Data Hiding

To further reduce the transmission risk the data hiding techniques such as Steganography is used to hide the noise share during the transmission. Steganography is a technique to hide information inside information which will secure the secrecy of transmission

The input of the encryption process is secrete image and natural images and we get noise like share at the output as shown in Fig.3(a). Exact reverse procedure happens at decryption as shown in Fig.3(b).

## 5. CONCLUSION

We conclude that the Visual secret sharing using natural images is more secure as it uses the only one noise-like share and innocuous natural shares which are transmitted using different carrier media so that the interception risk is minimized. Also the possible ways are used to hide the noise like share which reduces the transmission risk problem. So this proposed system is highly effective solution for reducing the transmission risk problem.

## ACKNOWLEGEMENT

We are very much thankful to our guide Prof. Jagruti Wagh for her guidance, continuous support and suggestions which greatly contribute to our paper. We sincerely thank our Head of Department (Comp.) Prof. H. K. Khanuja for her encouragement throughout our paper preparation. We are also gratefully thank you to our respected Principal Dr. S. M. Deshpande for his co-operation and support despite of his busy schedule. Last but not least we are thankful to all our computer department staff members for providing such an excellent environment to undergo this paper.

## REFERENCES

*[1]. M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology,vol. 950. New York, NY, USA: Springer-Verlag, 1995.*

*[2]. R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia,"Incrementing visual cryptography using random grids," Opt. Commun.,vol. 283, no. 21, pp. 4242–4249, Nov. 2010.*

*[3]. P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," IEEE Trans. Inf. ForensicsSecurity, vol. 6, no. 3, pp. 992–1001, Sep. 2011.*

*[4]. K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," IEEETrans. Image Process., vol. 22, no. 10, pp. 3830–3841, Oct. 2013.*

*[5]. N. Askari, H.M. Heys, and C.R. Moloney," AN EXTENDED VISUAL CRYPTOGRAPHY SCHEME WITHOUT PIXEL EXPANSION FOR HALFTONE IMAGES", 26th IEEE Canadian Conference Of Electrical And Computer Engineering (CCECE),2013.*

*[6]. Maneesh Kumar, Sourav Mukhopadhyay "Visual Cryptography for Black and White Images", International Journal of Information and Computation Technology. Vol 3,pp. 1149-1154,November 11 2013.*

*[7]. Kai-Hui Lee and Pei-Ling Chiu," Digital Image Sharing by Diverse Image Media", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014.*